



Deputy Director  
for Administration

DDA 87-2553X  
02 December 1987

NOTE FOR: Office of General Counsel

SUBJECT: Questions Regarding SF 189

The attached letter from Steven Garfinkel, Director, Information Security Oversight Office, is forwarded for your action. Please note that a response is requested by COB 8 December. We have requested our Office of Security to provide you their input to the questions by noon on 4 December. We are requesting that your response be to the DDA by COB 7 December.



*fa* William F. Donnelly

Att:  
A/S

cc: OCA for info.

STAT



BY MESSENGER

November 30, 1987

Dear Mr. Donnelly:

As a follow-up to a hearing he chaired on October 15, 1987, Congressman Gerry Sikorski, Chairman of the Subcommittee on Human Resources of the House Committee on Post Office and Civil Service, has submitted written questions to the Information Security Oversight Office (ISOO) regarding the Standard Form 189, "Classified Information Nondisclosure Agreement." Congressman Sikorski asked that he receive responses to those questions by December 14. The National Security Council (NSC) has orally directed ISOO that we are to do our best to meet that deadline for as many questions as possible, noting that our answers must first be coordinated through the NSC and the Department of Justice, which is representing us in litigation over the SF 189.

Answering a number of these questions fully will require the input of agencies other than ISOO. We enclose copies of those questions for which we believe your input is necessary. We have annotated these questions by noting beside them those agencies that should provide input to ISOO. In order for ISOO to prepare the final answers and coordinate them, we must have your input no later than close of business on Tuesday, December 8. If you cannot meet this deadline for a question, we must know the particulars, including why you cannot provide input by that time and the time by which the input will be provided. Please do not mail your responses. Phone your ISOO liaison to coordinate delivery.

Sincerely,

(signed) Steven Garfinkel

Steven Garfinkel  
Director

Mr. William F. Donnelly  
Deputy Director for Administration  
Central Intelligence Agency  
Washington, DC 20505

Enclosure

GERRY SIKORSKI, MINNESOTA, CHAIRMAN  
GUS YATRON, PENNSYLVANIA    DAN BURTON, INDIANA  
FRANK McCLOSKEY, INDIANA    BENJAMIN A. GILMAN, NEW YORK

## U.S. House of Representatives

COMMITTEE ON POST OFFICE AND CIVIL SERVICE  
SUBCOMMITTEE ON HUMAN RESOURCES  
406 CANNON HOUSE OFFICE BUILDING  
Washington, DC 20515

TELEPHONE (202) 225-2821

November 13, 1987

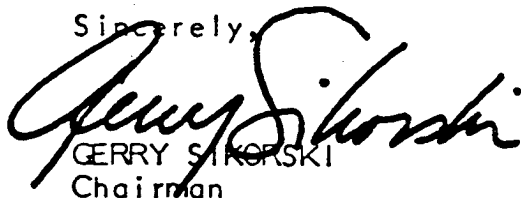
Mr. Steven Garfinkel  
Director  
Information Security Oversight Office  
General Services Administration  
Washington, D.C. 20405

Dear Mr. Garfinkel:

Enclosed please find the questions concerning Standard Form 189 that I mentioned to you during the the Subcommittee's October 15, 1987, hearing. As I noted then, time constraints prevented me from raising these questions with you personally. However, your answers to them will be a very important part of the Subcommittee's ongoing examination of the use of nondisclosure forms.

Please provide the Subcommittee with appropriate responses by December 14, 1987. If you have any questions regarding this request, please contact Mr. Courtney Ward or Ms. Rebecca Tillet of the Subcommittee staff at 225-2821. I look forward to your prompt reply.

Sincerely,



GERRY SIKORSKI  
Chairman  
Subcommittee on Human Resources

GS/rt  
Enclosure

19

Z

## Questions Regarding Standard Form 189

### I. BASIS AND NEED FOR NONDISCLOSURE AGREEMENTS

INPUT

1. Please explain what national security concerns addressed by SF 189 would remain unsolved if employees holding security clearances instead were required to sign the following agreement: "I am aware of my duty to protect classified information, have been trained in my responsibilities to protect classified information and pledge to honor my duty to protect classified information."

ISOO  
Justice

2. What specific statutes have failed to adequately protect classified information? Please reference any unsuccessful attempted prosecutions, or the facts of any case that the Department of Justice wanted to prosecute in this area but declined due to weaknesses in existing statutes.

Justice  
ISOO

3. What legislative proposals has the administration made to plug these statutory loopholes? Please be specific in matching particular provisions of any proposed legislation to the individual loopholes that have frustrated prosecutions or other personnel actions.

Justice  
OMB

4. In the absence of SF 189 why can't any agency take an adverse action on the grounds of impeding the efficiency of the service, against an employee who improperly discloses sensitive information?

Justice  
OPM  
ISOO

5. What and how many national security leaks have occurred due to the release of information that is classifiable but not classified? Please specify the definition of classifiable upon which you base this answer.

ISOO  
CIA  
Justice

6. Who in the National Security Council (NSC) authored SF 189? Who in the NSC reviewed and approved the nondisclosure agreement? Who in the Department of Justice reviewed the form before and since its release?

ISOO  
NSC  
Justice

7. What public interest groups participated in the discussions preceding the issuance of SF 189? Did these groups review a summary of principles for a valid nondisclosure agreement or the specific language of SF 189?

ISOO

8. What are the other, stronger nondisclosure agreements that have been upheld by the courts? Please provide legal citations for any such precedents.

Justice  
CIA

### II. IMPLEMENTATION OF SF 189

1. Please list all agencies with employees who are required to sign SF 189.

ISOO

2. How many employees without security clearances have signed SF 189? What was the legal authority to require signatures by employees without security clearances? Is this practice still continuing?

INPUT  
All  
agencies

3. Were Oliver North, Fawn Hall, or William Casey at any time required to sign a nondisclosure agreement? If not, why not? If so, what agreement, and what enforcement actions have been taken, or investigations opened, to hold Messrs. Casey and North and Ms. Hall, accountable for their potential violations of the nondisclosure agreement they signed?

NSC  
CIA  
DOD

4. Do the explanations for SF 189 in the question and answer training pamphlet, DOD 5200.1-PH-1, have the force of law? In other words, is it a valid legal defense for an employee charged with SF 189 violations to prove that s/he relied on guidance from that training pamphlet? If not, why not? If not, please list all other non-binding explanatory materials that have been released, and upon which employees are not entitled to assert reliance to interpret the contract.

DOD  
Justice  
ISOO

5. Recently, through the Federal Register and correspondence with Congress, ISOO has issued a series of clarifying rules, notices and modifications to SF 189. To the extent that these or other new rules and/or notices modify the meaning of SF 189, can they ever be rescinded or further revised? If so, what procedure is necessary for modifications to be legally binding on a permanent basis? Please describe the boundary for what changes are permissible to SF 189s that already have been signed.

ISOO  
Justice

6. What retraining has the Administration initiated to correspond with all the recent clarifications? Has the retraining been consistently implemented for all agencies and employees covered by SF 189?

All  
agencies

7. If there has been no retraining to teach civil servants the impact of the new "clarifying" rules and modifications for SF 189, is any planned? Under what circumstances would additional training be necessary?

All  
agencies

8. The ISOO has stated that liability for release of unclassified information is limited to information being processed under section 1.1(c) of Executive Order 12356 for a final decision on classification status. Is an employee liable for release of unclassified but classifiable information if there is no final decision within 30 days on classification status, as required by section 1.1(c)?

ISOO  
Justice

9. Please describe fully the procedures to implement section 1.6(a) of E.O. 12356, under which employees may challenge the status of information that they believe has been improperly classified in order to conceal illegality or other misconduct.

All  
agencies  
ISOO

10. How many challenges of allegedly improper classifications have been filed under section 1.6(a) of E.O. 12356? How many classification decisions have been upheld and how many have been reversed? What is the range and average times to make decisions under section 1.6(a)?

INPUT  
All  
agencies  
ISOO

### III. FLOW OF INFORMATION TO CONGRESS

1. What is the definition of a recipient who is "authorized" to receive classifiable information? What is the legal basis for the definition? Please fully describe the distinctions between the status of being "cleared" for receipt of classified information and being "authorized" for receipt of classified or classifiable information, as well as the legal basis for that distinction. Who, if anyone, is inherently "authorized" by virtue of his or her position to receive information covered under SF 189?

ISOO  
Justice

2. Are all Members of Congress or members of their staffs who sign SF 189s or analogous nondisclosure agreements inherently "authorized" to receive information covered by the agreement? If not, why not? Are all executive branch employees who sign SF 189s "authorized" to receive information covered by the nondisclosure agreement?

Justice  
ISOO

3. What is the definition of congressional "need to know"? Does information that the employee reasonably believes evidences illegality, mismanagement, abuse of authority, gross waste or a substantial and specific danger to the public health or safety fall within this "need to know" category.

Justice  
ISOO

4. Who determines whether Members of Congress or any other potential recipient has a "need to know" classifiable information and what written criteria or guidelines are applied to make this determination. (Please identify all individuals in all covered agencies, by office name and individual name and title, who have this responsibility.)

Justice  
ISOO  
All  
agencies

5. What is the legal basis for making decisions about who is "authorized" and has a "need to know" classifiable information?

Justice  
ISOO

6. Does an employee incur liability for making disclosures to Congress under 5 USC 7211 or 18 USC 1505, if the relevant individual or agency office determined that the congressional recipient was not authorized to receive the information under SF 189?

Justice

### IV. THE TERM "CLASSIFIABLE"

1. Don't the definitions of "classified" in E.O. 12356 and the Industrial Security Manual include proper designation of the information's classified status as a necessary element in the definition of that term? What is the specific legal basis for the ISOO's contention that information can have the legal status

ISOO  
Justice  
DOD  
CIA

of being classified without any markings to that effect?

INPUT

2. What are the laws that permit or require interim marking of documents that have not yet received a final decision on classification status? Is anyone prohibited from marking a document with the notation "Classification determination pending. Protect as though classified. (CONFIDENTIAL, SECRET, or TOP SECRET)," as described on page 49 of the Industrial Security Manual? If not, shouldn't all information be marked with either an interim or final classification status when relevant? If there are marking restrictions, what are all the legal options for employees who generate classified data but do not have the authority to mark its interim or final status?

Justice  
ISOO  
DOD  
CIA

3. Under what circumstances can employees with security clearances mark data as classified information that they generate or discover?

ISOO

4. What liability is incurred by employees without security clearances who disclose classifiable information to unauthorized persons? Has this system of accountability been effective? If not, why isn't that group also required to sign SF 189?

Justice  
ISOO

5. What liability is incurred by employees who fail to mark information as classified under their interim or final authority?

ISOO  
Justice

6. Has the ISOO analyzed the comparative problem of leaks of classified versus classifiable information by civil servants with security clearances and, separately, by employees without security clearances? If not, could such an analysis be performed with existing data?

ISOO  
CIA

7. Which laws require civil servants to challenge what they believe are improper decisions to classify information?

ISOC  
Justice  
DOD

8. Do those same laws require civil servants to challenge what they believe are improper decisions to deem information "classifiable"? If so, please describe the legal procedure to challenge improper "classifiable" decisions. Please include all relevant legal citations in your response.

ISOO  
Justice  
DOD

9. Although contractors do not make original classification decisions, don't they generate data that becomes classified? Shouldn't the justification for the "classifiability" concept, i.e. that the data is in the process of receiving a final classification decision, apply to contractor employees far more frequently than to civil servants with security clearances? Why are contractor employees held to a lesser standard of liability than civil servants?

DOD  
ISOO

10. Has ISOO analyzed the comparative problem of leaks of classifiable versus classified information by civil service employees and, separately, by contractor employees. If not, could such an analysis be performed with existing data.

ISOO  
CIA  
DOD

V. INDIRECT DISCLOSURES

INPUT

1. Is there liability under SF 189 for an employee who discloses classified or classifiable information to a co-worker, if the employee should have known that the co-worker might disclose information to a congressional office that is cleared to receive classified information but not authorized to receive it?

ISOO  
JusticVI. EFFECT ON EMPLOYEES

1. Does the administration stand by the quotations attributed to Mr. Garfinkel in an August 12, 1987, United Press International article, as follows: "An agency manager who believes that an employee has released classified or classifiable information can revoke or suspend his security clearance, or fire, suspend, demote or reprimand him. The manager may seek a legal opinion from the Justice Department or agency counsel before taking action but is not required to do so." If the answer is "yes," does it apply to civil servants generally, or only to those who have signed SF 189 or another nondisclosure agreement?

ISOO  
NSC  
Justic  
OPM

2. Please provide the names of the 24 employees with security clearances who refused to sign an SF 189, the agencies with which they are/were affiliated, and the dates they refused to sign. Have any employees without security clearances refused to sign an SF 189?

AF, DL  
GSA  
NASA  
NRC  
SEC

3. What happened to the 24 employees with security clearances who refused to sign SF 189? Were their clearances revoked? Please disclose and explain all subsequent job consequences for these employees, such as transfers, reassignments, or demotion.

AF, DL  
GSA  
NASA  
NRC  
SEC

4. How many employees have been denied security clearances due in whole or in part to their failure to sign SF 189?

All  
agencies

5. How many employees have been put on an ineligible list for promotions due in whole or in part to their failure to sign SF 189?

All  
agenciesVII. EMPLOYEE RIGHTS

1. What is the range of due process rights for employees at various agencies who face disciplinary action, revocation of security clearance or denial of security clearance for failing to sign SF 189? Please provide legal citations for the appropriate regulations at each covered agency as well as the procedures available for the employee to challenge these three potential consequences.

All  
agencies



1A. Please provide the same information for an employee charged with violating SF 189.

INPUT  
All  
agencies

2. Will the administration take any different action against an employee who has not signed SF 189 but discloses classifiable information to an unauthorized person, compared to an employee who has signed SF 189 and makes a prohibited disclosure? If so, please explain the differences.

ISOO  
Justice

#### VIII. CONTRACT ISSUES

1. Assuming that SF 189 is a valid contract, how do the numerous unilateral changes made over the past six months affect its legality?

ISOO  
Justice

#### IX. CONFLICT OF LAWS

1. Under SF 189, is an employee liable for making disclosures of information otherwise protected by the whistleblower statute (5 USC 2302(b)(8)) when the Executive begins the process of marking the information classified after the whistleblower exposes misconduct? Put another way, is all unmarked information whose disclosure is not prohibited under other congressional statutes protected despite SF 189, if the whistleblowing employee reasonably believes the information evidences illegality or other misconduct covered under 5 USC 2302(b)(8)? Do disclosures of unmarked but classifiable information disqualify an employee from protection under the whistleblower statute?

Justice  
OPM  
ISOO

2. Please list the legal duties that Federal employees have to disclose certain information (i.e. Employee Code of Ethics). When there is a conflict between a statutory duty to disclose and SF 189, which prevails?

Justice  
OPM

3. Under section 552(b)(1) of the Freedom of Information Act Executive Branch employees cannot withhold improperly classified data merely because it is marked as classified. Are employees who sign SF 189 required to withhold information that they know or reasonably should know is improperly classified? If so, please provide all legal references in support of this contention.

ISOO  
Justice

#### X. CLASSIFICATION GUIDE

1. For each system, program, plan, or project involving classified information, there is an information security guide. The Index to these guides lists over 3,700 individual guides. The Index is 370 pages and the individual guides total hundreds if not thousands of pages. Is it the position of ISOO that all

ISOO  
DOD

INPUT

individuals with security clearances are chargeable with actual or constructive knowledge of all of the information relating to the classification of information contained in these guides?

2. To whom is the Index of Security Classification Guides made available? DOD

3. What is the procedure by which users of the Classification Guides may challenge security classifications reflected in the guides? All original classifying agencies

4. Who is the final authority on the proper interpretation and application of a Classification Guide? All original classifying agencies